



FORM PTO-1449 INFORMATION DISCLOSURE CITATION				Attorney Docket: 2455-4581US1		Serial No.: Unassigned	
				Applicant: Gerrit Bleumer			
				Filing Date: October 23, 2000		Group Art Unit: Unassigned 2137	
U.S. PATENT DOCUMENTS							
Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date
PK	AA	4,926,480	05/15/90	Chaum	380	25	11-23-87
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
FOREIGN PATENT DOCUMENTS							
	AL						
	AM						
	AN						
	AO						
	AP						
OTHER DOCUMENTS (Including Author, Title, Date, etc.)							
PK	1	Matt Blaze, Gerrit Bleumer, Martin Strauss: Divertible Protocols and Atomic Proxy Cryptography; Eurocrypt '98, LNCS 1403, Springer-Verlag, Berlin 1998, 127-144.					
	2	Gerrit Bleumer: Biometric yet Privacy Protecting Person Authentication; Information Hiding Workshop '98, LNCS 1525, Springer-Verlag, Berlin 1998, 101-112.					
	3	Stefan Brands: An Efficient Off-line Electronic Cash System Based On The Representation Problem; Centrum voor Wiskunde en Informatica, Computer Science/Departement of Algorithmics and Architecture, Report CS-R9323, March 1993.					
	4	Stefan Brands: Untraceable Off-line Cash in Wallet with Observers; Crypto '93, LNCS 773, Springer-Verlag, Berlin 1994, 302-318.					

JCE41 U.S. P. 3

09/694779



FORM PTO-1449 <u>INFORMATION DISCLOSURE CITATION</u>		Attorney Docket: 2455-4581US1	Serial No.: Unassigned 09/694,779
		Applicant: Gerrit Bleumer	
		Filing Date: October 23, 2000	Group Art Unit: Unassigned 2137
	5	Ernest Brickell, Peter Gemmell, David Kravitz: Trustee-based racing Extensions to Anonymous Cash and the Making of Anonymous Change; 6 th ACM-SIAM Symposium on Discrete Algorithms (SODA)1995, ACM Press, New York 1995, 457-466.	
	6	David Chaum: Blind Signature System; Crypto '83, Plenum Press, New York 1984, 153.	
	7	David Chaum: A New Paradigm for Individuals in the Information Age; 1984 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, Washington 1984, 99-103.	
	8	David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985)1030-1044.	
	9	David Chaum: Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms; Auscrypt '90, LNCS 453, Springer-Verlag, Berlin 1990, 246-264.	
	10	David Chaum, Amos Fiat, Moni Naor: Untraceable Electronic Cash; Crypto '88, LNCS 403, Springer-Verlag, Berlin 1990, 319-327.	
	11	David Chaum, Torben Pryds Pedersen: Wallet Databases with Observers. Crypto '92, LNCS 740, Springer-Verlag, Berlin 1993, 89-105.	
	12	Jan L.Camenisch, Jean-Marc Piveteau, Markus A. Stadler: An Efficient Electronic Payment System Protecting Privacy; ESORICS 94 (Third European Symposium on Research in Computer Security), Brighton, LNCS 875, Springer-Verlag, Berlin 1994, 207-215.	
	13	Jan L. Camenisch, Jean-Marc Piveteau, Markus A. Stadler: Blind Signatures Based on the Discrete Logarithm Problem; Eurocrypt '94, LNCS 950, Springer-Verlag, Berlin 1995, 428-432.	
	14	Taher ElGamal: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms; IEEE Transactions on Information Theory 31/4 (1985)469-472.	
	15	Niels Ferguson: Single Term Off-Line Coins; Eurocrypt '93, LNCS 765, Springer-Verlag, Berlin 1994, 318-328.	
	16	Amos Fiat, Adi Shamir: How to Prove Yourself: Practical Solutions to Identification and Signature Problems; Crypto 86, LNCS 263, Springer-Verlag, Berlin 1987, 186-194.	
	17	Yair Frankel, Yiannis Tsiounis, Moti Yung: "Indirect Discourse Proofs": Achieving Efficient Fair Off-Line E-cash; Asia crypt '96, LNCS 1163, Springer-Verlag, Berlin 1996, 286-300.	
	18	Matthew Franklin, Moti Yung: Secure and Efficient Off-Line Digital Money; 20th International Colloquium on Automata, Languages and Programming (ICALP), LNCS 700, Springer-Verlag, Berlin 1993, 265-276.	
	19	Shafi Goldwasser, Silvio Micali, Ronald L. Rivest: A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks; SIAM Journal on Computing 17/2 (1988)281-308.	
	20	Andrew M. Odlyzko: Designs, Codes, and Cryptography (1999). To appear. http://www.research.att.com/amo/doc/complete.html	

FORM PTO-1449 <u>INFORMATION DISCLOSURE CITATION</u>		Attorney Docket: 2455-4581US1	Serial No.: Unassigned 09/694,779
		Applicant: Gerrit Bleumer	
		Filing Date: October 23, 2000	Group Art Unit: Unassigned
PK	21	David Pointcheval, Jacques Stern: Provably Secure Blind Signature Schemes; Asiacrypt '96, LNCS 1163, Springer-Verlag, Berlin 1996, 252-265.	
	22	David Pointcheval, Jacques Stern: New Blind Signatures Equivalent to Factorization; 4th ACM Conference on Computer and Communications Security, ACM-Press, New York 1997, 92-99.	
	23	Birgit Pfitzmann, Ahmad-Reza Sadeghi: Coin-Based Anonymous Finger-printing; To appear at Eurocrypt '99, Springer-Verlag, Berlin 1999.	
	24	Cristian Radu, Ren Govaerts, Joos Vandewalle: Efficient electronic cash with restricted privacy; Financial Cryptography '97, Springer-Verlag, Berlin, 57-69.	
	25	Markus Stadler, Jean-Marc Piveteau, Jan Camenisch: Fair Blind Signatures; Eurocrypt '95, LNCS 921, Springer-Verlag, Berlin 1995, 209-219.	
Examiner		Date Considered	
Paul Salahn		8/6/04	
EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.			